FortiExtender Release Notes

VERSION v3.2

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

11/15/2017

FortiExtender v3.2 Release Notes

36-320-308943-20171113

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-11-10	Initial release of v3.2 build 0316. Major release with bug fixes for FEXT-40D-AMEU product introduction.

Introduction

This document provides the following information for FortiExtender build 0316:

For more information on upgrading your FortiExtender device, see the *FortiExtender Administration Guide.*

Supported Models

FortiExtender supports the following models on GA 3.0 build 69 or above: FortiExtender-20D, FortiExtender-40D-INTL, and FortiExtender-40D-NAM.

FortiExtender-40D-AMEU is being newly introduced starting with GA 3.2 build 316.

All built-in modem models can be upgraded with compatible operator specific modem firmware.

What's new in FortiExtender v3.2

Apart from bug fixes, there are no changes in terms of configuration and features offered by the variants of FortiExtender-40D. The main difference being that FortiExtender-40D-AMEU uses a Sierra EM7455 modem that's capable of operating in North America and Europe alike with LTE-A technology, whereas the FortiExtender-40D-NAM and the FortiExtender-40D-INTL use modems Sierra EM7355 and EM7305 capable of LTE respectively. Additionally, the FortiExtender-40D-AMEU supports the GPS capabililty wherein the GPS coordinates get syslog'ed via the FortiGate.

Configuration Help

FortiGate CLI Configuration

If an APN were to be configured from the FortiGate this release mandates the configuration of the APN in the format "CarrierName:APN". The example below shows the Carrier set to Verizon and APN set to *vzwinternet*.

```
config extender-controller extender
```

```
edit FX04DN4N16000233
      set access-point-name "Verizon:vzwinternet"
      set ppp-username user
      set ppp-password 123
      set ppp-auth-protocol auto
   end
```

FortiExtender-20D CLI Configuration

1. Configuring APN from the FortiExtender-20D CLI which can also help initiate the Cellular Internet data connection despite the absence of theFortiGate APN config or for that matter the absence of the FortiGate itself while operating in bridge mode. The example below illustrates the Carrier set to *Verizon* and APN set to *vzwinternet*.

```
config modem sim-config
   add Verizon
      set Carrier Verizon
      set APN vzwinternet
      set USER user1
      set PWD 123
      set MODE auto
      set AUTH PAP
   end
```

2. Bridge mode configuration:

- Bridge Mode Enable

```
config system bridge-mode enable
   reboot
```

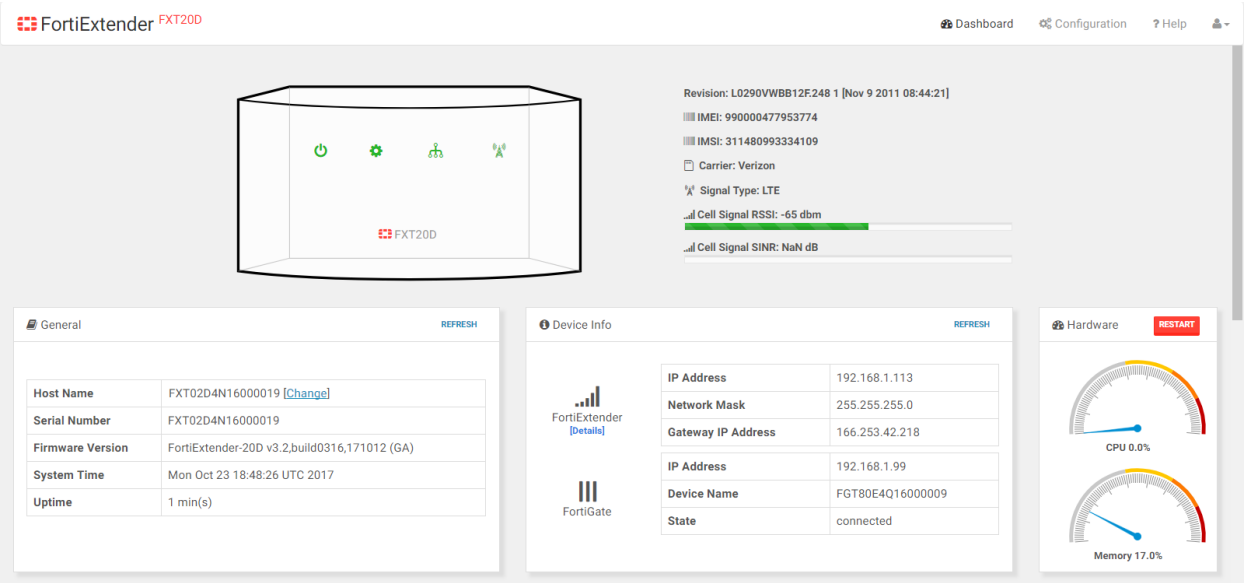
- Bridge Mode IP

```
config system bridge-mode-ip 192.168.100.2
      reboot
```

Note: The default IP adddress is 192.168.1.2, unless it is set by the user.

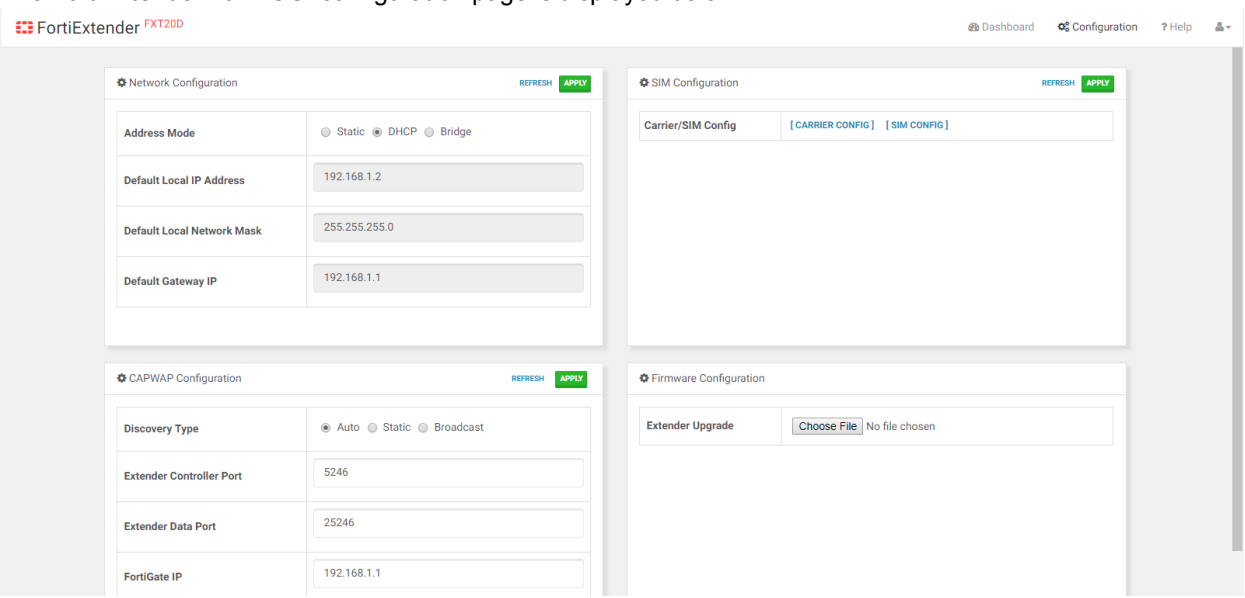
FortiExtender-20D GUI:

- The FortiExtender 20-D GUI home page is displayed below:



Home Page accessible at https port 60443 from both WAN and LAN sides with an exception being http accesssible only via LAN side.

- The FortiExtender 20-D GUI configuration page is displayed below:



FortiExtender-40D CLI Configuration

Static IPv6 Support: The FortiGate's FortiExtender linked interface can now be configured with the static IPv6 address and Gateway provided by the Wireless service provider. The FortiGate can now support IPv4 in DHCP mode and IPv6 in static mode simultaneously.

Most carriers in North America can work without any predefined configuration, but they may require APN configuration at times when authentication comes into play. Configuring APN, authentication, modem firmware to be used for any given operator on the FortiExtender-40D directly can also help initiate the Cellular Internet data connection without the need of any externally supplied configuration parameters. Currently, barring the APN and its related authentication parameters, most other parameters like the modem firmware to be used cannot be configured from the FortiGate.

1. Configuring APN and auth parameters with Verizon as an example, and APN as *vzwinternet*. Authentication parameters are to be set on a need basis only. Getting the Carrier Name right is instrumental in making the configuration work well.

```
config modem sim-config
   add Verizon
      set Carrier Verizon
      set APN vzwinternet
      set USER user1
      set PWD 123
      set MODE auto
      set AUTH PAP
end
```

2. Bridge mode configuration:

- Bridge Mode Enable

```
config system bridge-mode enable
   reboot
```

- Bridge Mode IP

```
config system bridge-mode-ip <x.x.x.x>
   reboot
```

3. Signal notification config

- Periodic

```
config modem setting
   set rssi-interval 30  <Periodically reports detailed signal statistics to FortiGate.>
end
```

- Threshold Based

```
config modem setting
   set rssi-threshold 20 <Reports RSSI fluctuations over 20dBm (default is 10dBm).>
```

4. Monitor data-usage statistics

```
get modem data-usage
```

5. Configuring a data plan

```
config modem sim-config
   add 1
      set Slot sim1
      set Data-plan 1000; 13; enable <Data in MB (100- 102400), Billing Date (1-31), overage
          (enable/disable)>
   end
```

6) Enabling the sim-switch while using two sim cards

```
config modem setting
```

```
set sim-switch enable <Enables selection of a sim based on configuration (see Step 7)>
end
```

7)Setting the SIM switch criteria

- Based on disconnections when the sim-switch is enabled (see Step 6).

```
config modem setting
   set switch-on-disconnect 4;600 <No. of disconnects (1-100); evaluation period in seconds (600-18000)>
   end
```

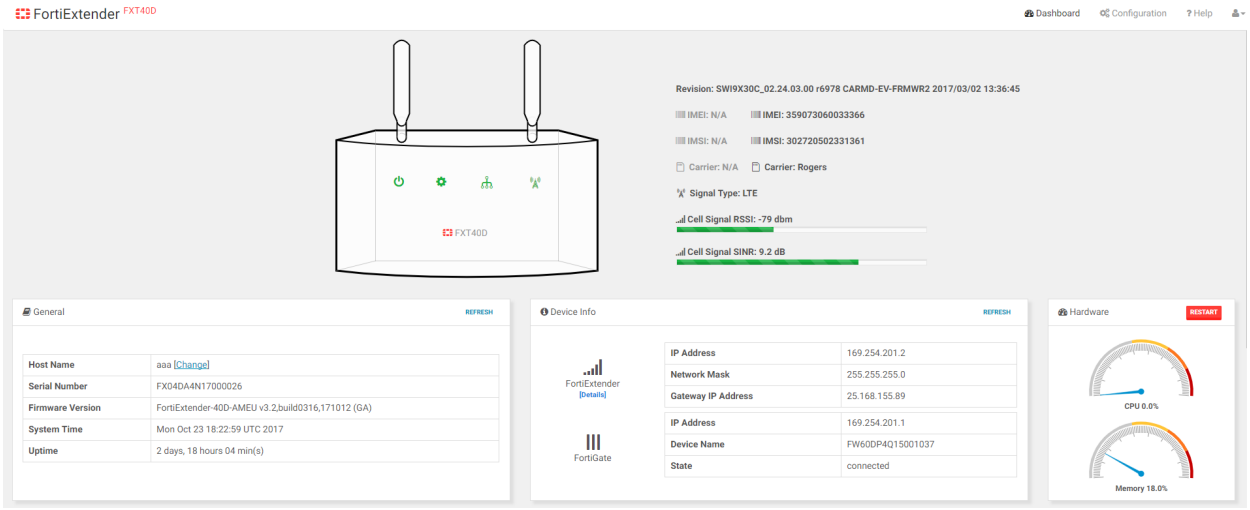
- Based on Signal Quality when sim-switch is enabled (see Step 6)

```
config modem sim-config
   add 1
      set Slot sim1
      set Signal -95;600 <Min RSSI value in dBm (-100 to -50); evaluation period in seconds (600-18000)>
      end
```

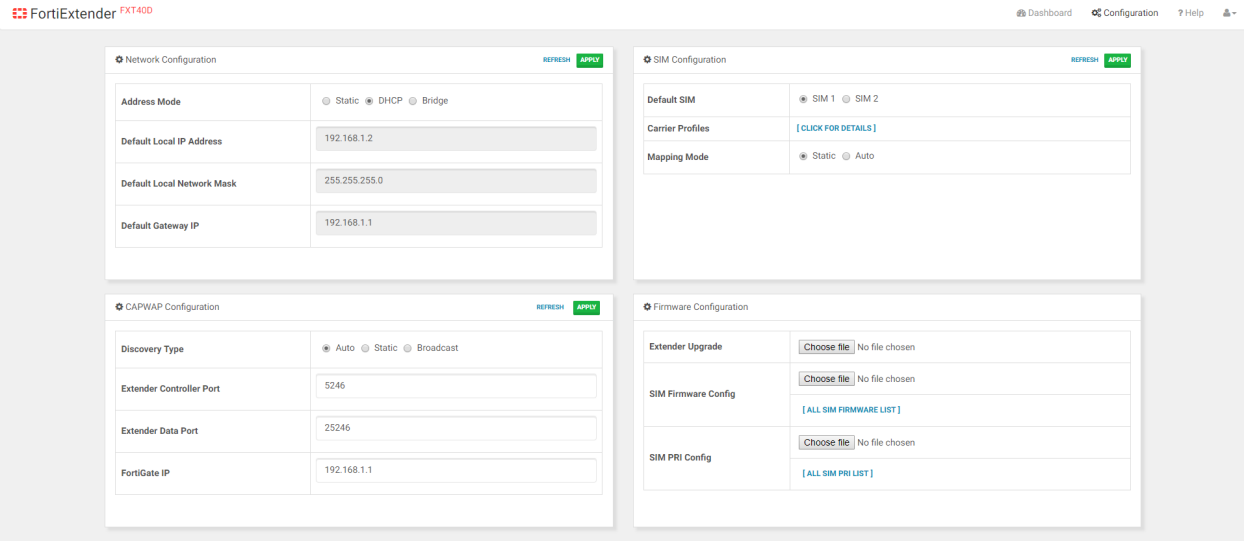
- Based on Data Usage

Please refer to Step 5. Available regardless of the sim-switch parameter being enabled or not.

- The new FortiExtender-40D GUI home page is displayed below:



- The new FortiExtender-40D configuration page is displayed below:



- The new FortiExtender-40D GUI signal statistics is displayed below:

Upgrade Information

Upgrading to FortiExtender v3.2

FortiExtender-20D and FortiExtender-40D are capable of operating on v3.0.0 GA build 69 and above.

The built-in modems residing in FEXT-40D-NAM and FEXT-40D-INTL can also be upgraded with compatible operator specific modem firmware.

Firmware upgrade procedure

Firmware Information:

The Sierra EM7355/EM7305/EM7455 Modem Software comprises of two files:

- A PRL file with the file name ending "*.nvu*"
- A firmware file with the ending "*.cwe*"

Both files are required to be flashed onto the Modem to connect to the operator of your choice.

Upgrade instructions and the MODEM firmware have been uploaded to Fortinet Customer Support site in the download directory under: "…/FortiGate/v5.00/5.4/Sierra-Wireless-3G4G-MODEM-Upgrade/".

Firmware upgrade via the FortiExtender GUI:

1. Login to the web GUI of the FortiExtender with the default credentials. For the username enter *admin* and leave the password blank.
2. In the FortiExtender GUI from in the bottom right corner, click **Sim Firmware Config**.
3. Select the corresponding firmware ending in ".cwe" and flash it.
4. Then, select the corresponding PRI, i.e. the ".nvu" file from **Sim PRI Config** and flash it.
5. After the upgrade is completed, click on the **RESTART** button and confirm with a **YES**.
6. This procedure can take 3 to 5 minutes to finish. Wait for the reboot and make sure the SIM slot is holding the desired SIM.

Firmware mapping to an operator

Once a firmware is uploaded it has to be linked to a Wireless carrier/ operator. Typically a SIM has an IMSI number. The first 6 digits constitute the MCC and MNC will help FortiExtender determine the Carrier of choice most of the time. Otherwise a new entry needs to be created.

Refer to the CLI Help Section for configuration details.

Product Integration and Support

Modes of operation

FortiExtender supports Connected UTM and Standalone modes of operation.

Connected UTM mode

This is the default mode of operation where the FortiGate provides centralized management of the FortiExtender infrastructure. In this mode the device discovers the FortiGate using the CAPWAP protocol and WAN traffic is tunneled to the FortiGate's wireless WAN virtual interface. For connect UTM mode, FortiGates must run FortiOS v5.2.0 or later.

FortiExtender v3.2 support

The following table lists FortiExtender product integration and support information.

FortiExtender 3.0.2 Support	
Web Browsers	Microsoft Internet Explorer versions 10 and 11 Mozilla Firefox version 33 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS/FortiOS Carrier	v5.2.0 and later
FortiManager	v5.0.7 and later v5.2.0 and later

USB modem support

The following tables list USB modems that are supported for various models.

FortiExtender-20D

The following table lists USB modems that are supported by the FortiExtender-20D:

Brand	Modem Model	Operator / Area
Netgear	340U	AT&T (USA)
Sprint	341U	Sprint (USA)
Sierra	313	AT&T (USA)
Pantech	295	Verizon
ZTE	820B	Claro (Puerto Rico)
ZTE	MF683	T-Mobile
Novatel	MF620L	Verizon
Huawei	E398	Any GSM/LTE
Huawei	UMG1691	T-Mobile
Huawei	E173	Any GSM, 3G, HSPA network
Huawei	E3276	Any GSM/LTE
TPLINK	MA260	Any GSM/3G
TPLINK	MA180	Any GSM/3G
ZTE	K3520-Z	HSDPA, WCDMA
ZTE	K3563-Z	
ZTE	K3565-Z	HSDPA 3.6/0.38
ZTE	K3570-Z	HSDPA 3.6/0.38
ZTE	K3571-Z	HSDPA 7.2/0.38
ZTE	K4505-Z	HSPA+ 21.6/5.76
ZTE	K5006-Z	LTE CAT3
ZTE	MF30	HSDPA 7.2 HSUPA 5.76
ZTE	MF60	HSPA+ 21.6/5.76
ZTE	MF100	HSDPA 3.6/0.38
ZTE	MF110	HSDPA 7.2 HSUPA 5.76

Brand	Modem Model	Operator / Area
ZTE	MF112	HSDPA 7.2 HSUPA 2.0
ZTE	MF170	HSDPA 3.6/0.38
ZTE	MF190	HSDPA 7.2 HSUPA 2.0
ZTE	MF626	HSDPA 3.6/0.38
ZTE	MF627	HSDPA 7.2 HSUPA 5.76
ZTE	MF632	HSDPA 7.2 HSUPA 3.6
ZTE	MF633	HSDPA 7.2 HSUPA 5.76
ZTE	MF636	HSDPA 7.2 HSUPA 5.76
ZTE	MF637	HSDPA 7.2 HSUPA 5.76
ZTE	MF637U	HSDPA 7.2 HSUPA 5.76
ZTE	MF662	HSPA+ 21.6/5.76
ZTE	MF668	HSPA+ 21.6/5.76
ZTE	MF668A	HSPA+ 21.6/5.76
ZTE	MF669	HSPA+ 21.6/5.76
ZTE	MF680	DC-HSPA+ 42.2/5.76
ZTE	MF683	DC-HSPA+ 42.2/5.76
ZTE	MF820D	LTE CAT3
ZTE	MF821	LTE CAT3
ZTE	MF821D	LTE CAT3
ZTE	MF880	LTE CAT3
ZTE	MT505UP	HSUPA
ZTE	MT512HS	HSDPA 7.2 HSUPA 3.6
ZTE	MT8205	LTE CAT3
HUAWEI	B81	HSDPA 7.2 HSUPA 5.76

Brand	Modem Model	Operator / Area
HUAWEI	D33HW	HSPA+ 21.6/5.76
HUAWEI	D41HW	DC-HSPA+ 42.2/11.5
HUAWEI	E153	HSDPA 3.6/0.38
HUAWEI	E156G	HSDPA 3.6/0.38
HUAWEI	E171	HSDPA 7.2 HSUPA 5.76
HUAWEI	E173	HSDPA 7.2 HSUPA 5.76
HUAWEI	E180V	HSDPA 7.2 HSUPA 5.76
HUAWEI	E200	HSDPA 3.6
HUAWEI	E261	HSDPA 7.2 HSUPA 5.76
HUAWEI	E270+	HSPA+ 21.6/5.76
HUAWEI	E303F	HSPA+ 21.6/5.76
HUAWEI	E352	HSPA+ 21.6/5.76
HUAWEI	E353W-u1	HSPA+ 21.6/5.76
HUAWEI	E367	DC-HSPA+ 28.8/5.76
HUAWEI	E372	DC-HSPA+ 42.2/5.76
HUAWEI	E389	LTE CAT3
HUAWEI	E392	LTE CAT3
HUAWEI	E398	LTE CAT3
HUAWEI	E398u-15	LTE CAT3
HUAWEI	E1552	HSDPA 3.6/0.38
HUAWEI	E1690	HSDPA 7.2 HSUPA 5.76
HUAWEI	E1691	HSDPA 7.2 HSUPA 5.76
HUAWEI	E1692	HSDPA 7.2 HSUPA 5.76
HUAWEI	E1731Bu-1	HSPA+ 21.6/5.76

Brand	Modem Model	Operator / Area
HUAWEI	E1762	HSDPA 7.2 HSUPA 5.76
HUAWEI	E1800	HSDPA 7.2 HSUPA 5.76
HUAWEI	E1815	HSPA+ 21.6/5.76
HUAWEI	E1820	HSPA+ 21.6/5.76
HUAWEI	E1823	HSPA+ 21.6/5.76
HUAWEI	E3131s-2	HSPA+ 21.6/5.76
HUAWEI	EC122	CDMA2000
HUAWEI	EC176-2	CDMA EV-DO Rev.A
HUAWEI	EC178	CDMA EV-DO Rev.A
HUAWEI	EC189	HSDPA 7.2 HSUPA 5.76
HUAWEI	EC306	HSPA+ 21.6/5.76
HUAWEI	EC1270	DC-HSPA+ 42.2/11.5
HUAWEI	Speedstick LTE	HSDPA 3.6/0.38

Resolved Issues

The following issues have been fixed in version v3.2. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
0443685	OBM option now enables Internet connectivity all the time.
0443177	The issues with the Internet session disconnecting upon de-authorizing FortiExtender have been fixed.
0421722	Factory reset now successfully erases the bridge mode configuration.

Known Issues

The following issues have been identified in v3.2. For inquires about a particular bug, please contact Customer Service & Support.

FortiExtender 40D:

Bug ID	Description
N/A	[AMEU] GPS triangulation takes at least 10 minutes.
N/A	[Sprint Cert] missing fields like DRC, PN code, PN offset, etc. in EVDO AT command output.
N/A	Physical insertion of a SIM requires a FortiExtender-40D power cycle.
N/A	Changing the FortiExtender mode from CAPWAP to VLAN or vice-versa requires a power cycle.

FortiExtender 20D:

Bug ID	Description
N/A	Physical insertion of a modem requires a FortiExtender-20D power cycle.
N/A	Changing the FortiExtender mode from CAPWAP to VLAN or vice-versa requires a power cycle.